Framing

NTIA Software Supply Chain Transparency

Éamonn Ó Muirí
https://flic.kr/p/46dsiz
https://creativecommons.org/licenses/by/2.0/legalcode

Framing Working Group

Managed with love and patience by co-chairs Michelle Jump and Art Manion

Meeting almost weekly since July 2018

- Fridays at 1400 EDT
- https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-framing

Framing concepts that apply to the entire multi-stakeholder process

Michelle Jump

MedSec LLC

Global Regulatory Advisor - Medical Device Cybersecurity

MichelleJump@medsec.com

Art Manion

Software Engineering Institute
CERT Coordination Center

Principle Engineer “/” Technical Manager

amanion@cert.org

Agenda

1. SBOM refresher
2. New draft documents
    1. Sharing and Exchanging SBOMs
    2. Software Identification Challenge and Guidance
3. Vulnerability status (“VEX”)
4. Expected upcoming work
    1. “VEX”
    2. Glossary
    3. Supplier identification?
    4. Health Care PoC collaboration, revise Framing phase 1 document?

Refresher: What is an SBOM?

Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)

https://tinyurl.com/y7s8ab3t

"An SBOM is effectively a nested inventory, a list of ingredients that make up software components."

Partial Table of Contents

2 What is an SBOM?

2.2 Baseline Component Information

2.4 Component Relationships

4 SBOM Processes

4.1 SBOM Creation: How

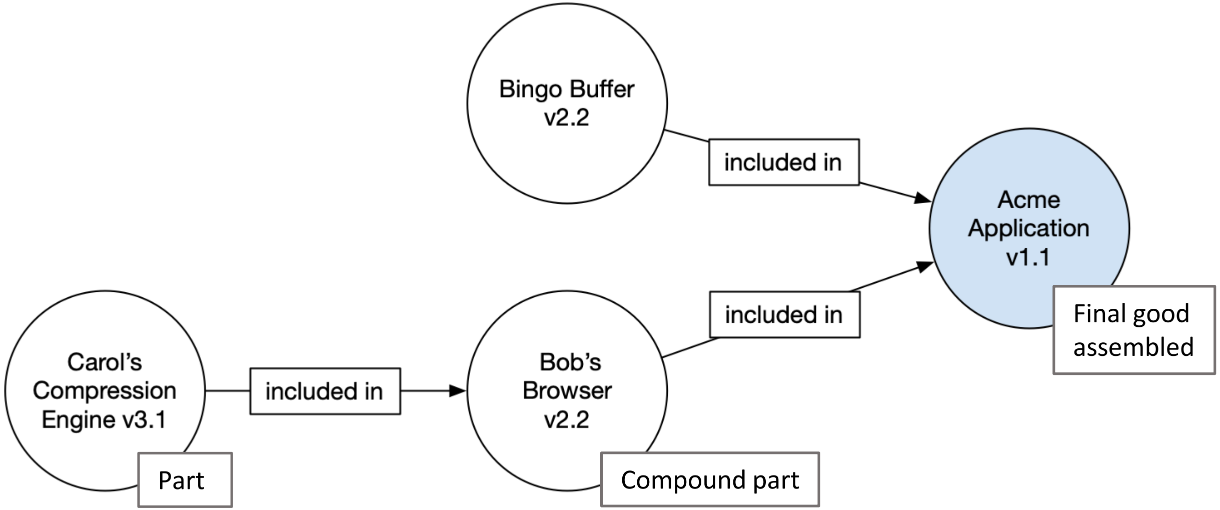
4.2 SBOM Creation: When

4.3 SBOM Exchange

4.4 Network Rules

4.6 Applications of SBOMs

5 Terminology



<table>
<tr><th>Component Name</th><th>Supplier Name</th><th>Version String</th><th>Author</th><th>Hash</th><th>UID</th><th>Relationship</th></tr>
<tr><td>Application</td><td>Acme</td><td>1.1</td><td>Acme</td><td>0x123</td><td>234</td><td>Self</td></tr>
<tr><td>|--- Browser</td><td>Bob</td><td>2.1</td><td>Bob</td><td>0x223</td><td>334</td><td>Included in</td></tr>
<tr><td>|--- Compression Engine</td><td>Carol</td><td>3.1</td><td>Acme</td><td>0x323</td><td>434</td><td>Included in</td></tr>
<tr><td>|--- Buffer</td><td>Bingo</td><td>2.2</td><td>Acme</td><td>0x423</td><td>534</td><td>Included in</td></tr>
</table>

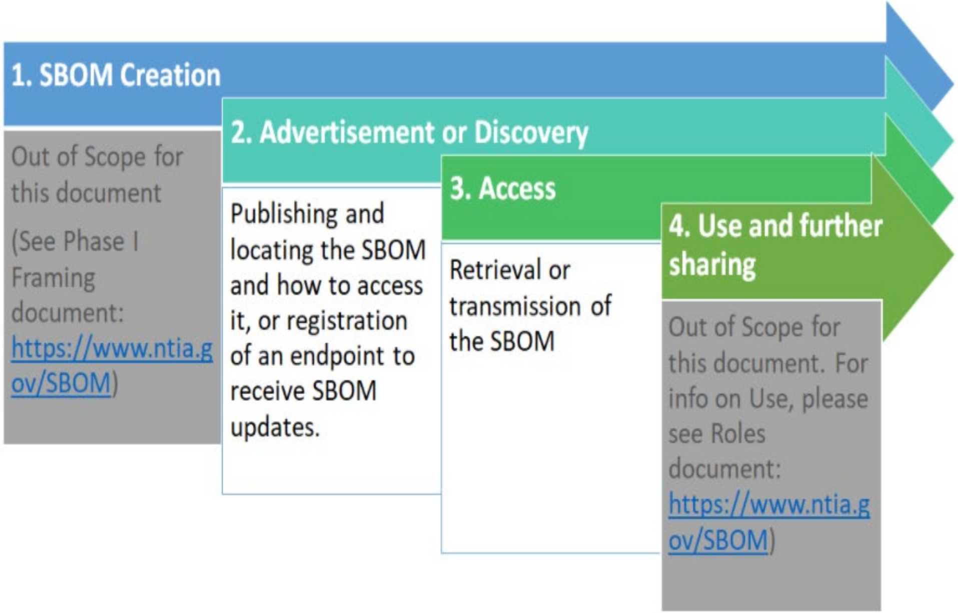
Draft paper: Sharing and Exchanging SBOMs

> "Transparency in the supply chain enables better risk decision-making for producers and consumers of software. This means that information about the underlying software components in a piece of software—a Software Bill of Material (SBOM)—should be accessible to the right entities at the right time."

Draft paper: Sharing and Exchanging SBOMs

Contents

- Terminology
- Advertisement and Discovery
- Access
- Status of This and Future Work



1. SBOM Creation

Out of Scope for this document

(See Phase I Framing document: https://www.ntia.gov/SBOM)

2. Advertisement or Discovery

Publishing and locating the SBOM and how to access it, or registration of an endpoint to receive SBOM updates.

3. Access

Retrieval or transmission of the SBOM

4. Use and further sharing

Out of Scope for this document. For info on Use, please see Roles document: https://www.ntia.gov/SBOM)

Link:

- https://tinyurl.com/y3cbn9zs

Draft paper: Sharing and Exchanging SBOMs

Key Process Points

- Advertisement and Discovery
  - How an author or a device informs consumers that an SBOM is available and how the SBOM is located
  - Example: URL, Manifest, Publish/Subscribe System
- Access (& Retrieval)
  - How the SBOM is obtained once it is discovered
  - Examples: directly via email, resident on device, on a server, part of software update

Draft paper: Software Identification Challenge and Guidance

> “Possibly the biggest single challenge to supply-chain transparency and the SBOM model is the difficulty in identifying software components globally... This paper captures some of the major challenges… and offers some guidance on how to address these challenges.”

Draft paper: Software Identification Challenge and Guidance

Contents

- Global Software Component Identification
- Name, Namespace, Identification
- Need for Component Identification
  - Primary SBOM Authorship
  - Secondary SBOM Authorship
  - SBOM Assembly
- Guidance for Component Identification
  - Preferred case – existing supplier/namespace
  - Alternate case – established software identity standard
- Supplier Identification

Link
https://tinyurl.com/y6pnhvke

Draft paper: Software Identification Challenge and Guidance

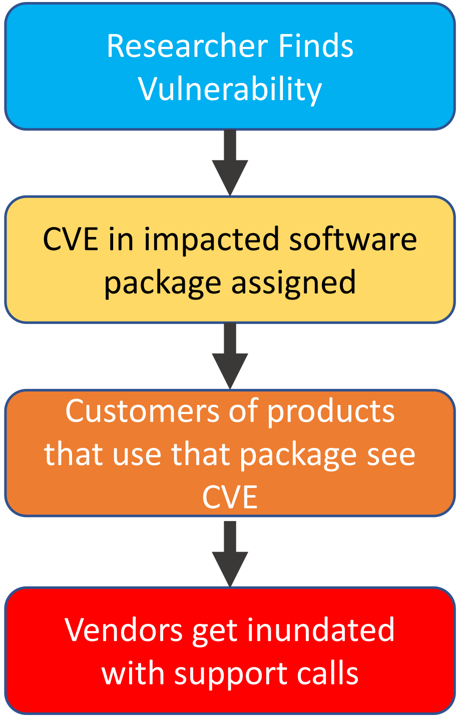
- Globally unique identification is hard
    - Many names, attributes, and identification systems
    - Format does not imply identity
- There is hope
    - Hierarchy, typed-relationships (think URLs, DNS, and aliases)
- High level guidance
    1. If existing identification system, use that
    2. Else choose from an existing system

“VEX:” Vulnerability (or exploitability) status

- To date has been called “VEX” (Vulnerability EXploitability)
  - Ironic that we’re having trouble with names?
  - The name is up for discussion
- Step 1: Draft description of the problem, needs, use cases
  - I see a vulnerable upstream component, what is my exposure?
  - https://tinyurl.com/yx8qvma7
- Step N: Solve problem
- Need to map vulnerability to component exists outside of SBOM

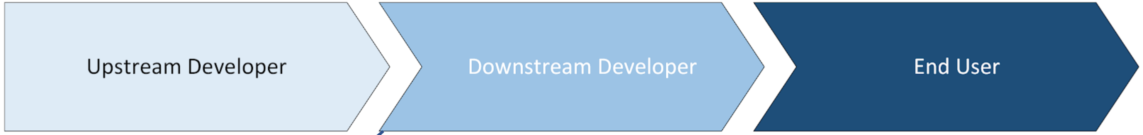
“VEX” Problems

- Users want to reduce risk from vulnerabilities – Vulnerability Management
  - Unknown, unpatched
- With SBOM, users know more about upstream components
  - Is upstream vulnerability inherited?
  - Now: Users ask suppliers
  - Future: Users answer their own questions
- Some users are also (downstream) suppliers



Researcher Finds Vulnerability
CVE in impacted software package assigned
Customers of products that use that package see CVE
Vendors get inundated with support calls

“VEX” business requirements and actors



Upstream Developer

Downstream Developer

End User

- Delivers components for use by others.
- Creates CVEs
- May create SBOMs

- Consumes and utilizes components created by others.
- May deliver a product to the end user or another downstream developer
- Creates CVEs
- Consumes upstream CVEs
- May create SBOMs
- May indicate Product vulnerability to upstream vulnerabilities
- Wants to minimize end user calls for non-affected Products

- Makes use of the Product
- Consumes CVE, SBOM, and VEX information
- Desire to understand their risk exposure
- Desire to minimize false positive vulnerabilities.

Interfaces

Information elements

“VEX” questions and next steps

- Do we have the actors correct?
- Do we have their motivations correct?
- We think next step is to survey what if anything is out there that provides necessary information elements and interfaces
    - (For example: maybe CycloneDX?)
- Otherwise, at least loosely describe information elements, and desired interfaces
- And what do we call *This?*

Requests

- Review draft documents, provide comments
- Interested in ongoing or upcoming work? Join us:
  - Fridays at 1400 EDT
  - Mailing list: https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-framing
  - Google Drive: https://tinyurl.com/yc3gajzz
- Should we be aware of, coordinating with other efforts?
- Have we identified important gaps from Phase 1?